Winner of the 2026 CNMT Essay Competition

Vulnerable Arteries: Protecting Critical Subsea Infrastructure and the RCN's Mandate

C.A.M. Al Wahi



Credit: Finnish Border Guard

Image of damage on the Balticconnector natural gas pipeline between Ingå, Finland, and Paldiski, Estonia, taken October 2023.

On 8 October 2023 the Balticconnector gas pipeline connecting Finland and Estonia ruptured, simultaneously severing a telecommunications cable running in the same corridor. Finnish investigators established that the Hong Kong-registered cargo vessel *NewNew Polar Bear* had dragged its anchor across the seabed. Almost three years on, the only criminal proceeding is against the ship's master in a Hong Kong court, a forum with no connection to the states that suffered the damage.[1] A year earlier, explosive charges shattered the Nord Stream 1 and 2 pipelines under the Baltic Sea. German prosecutors charged a Ukrainian national in July 2026, but a Polish court has refused to surrender a second suspect and no state has been held to account.[2] These two incidents share a defining characteristic: the actors responsible understood that attacking infrastructure below the surface yields maximum strategic effect at minimum legal and political risk.

These are proof-of-concept examples of a type of infrastructure warfare that is directly relevant to Canada's maritime approaches, cable corridors and offshore assets – and to a maritime security doctrine that is unprepared. The ocean floor, long treated as a passive substrata beneath the real business of naval power, has become contested geopolitical terrain.

This article argues that Canada must reconceptualize critical subsea infrastructure protection as a primary naval security mission, building an integrated 'seabed-to-space' maritime domain awareness framework that combines Royal Canadian Navy (RCN) capabilities, Canadian Coast Guard (CCG) assets, NATO cooperation, advanced underwater surveillance technologies and a coherent grey-zone deterrence doctrine. The argument is not that Canada must achieve undersea dominance, an ambition beyond any middle power, but that it must develop the detection, deterrence and response capacity appropriate to a state the geography of which places it at the intersection of the North Atlantic, the Arctic and the world's most consequential transatlantic cable corridors. (In the interest of brevity, this article focuses on the Atlantic and Arctic coasts of Canada, but the same arguments apply to the Pacific coast.)

The Strategic Significance of Subsea Infrastructure

Approximately 95% of international internet traffic transits more than 400 undersea cable systems spanning over 1.3 million kilometres (just over 800,000 miles) of ocean floor.[3] These cables carry not only commercial data but classified government communications, military messaging and financial operations. This is why the 2022 NATO Strategic Concept, still the alliance's capstone document, explicitly identified threats to critical infrastructure, including undersea systems, as a collective security challenge requiring an alliance response.[4] At the 2025 NATO meeting in the Hague, allies undertook to devote up to 1.5% of Gross Domestic Product (GDP) annually to protecting critical infrastructure and defending networks.[5] The disruption of a major trunk route would simultaneously

impair NATO command-and-control, civilian emergency communications and continental financial stability.

Canada's position within this architecture is consequential. Several transatlantic cable systems make landfall from Nova Scotia to Newfoundland, linking North American and European networks through landing stations that are geographically concentrated and inadequately monitored.[6] (The Pacific coast repeats the pattern in a different ocean.) The same stretch of Atlantic seabed underlies Canada's primary maritime approaches, the corridors through which any military threat to the continent would transit. The dual vulnerability, strategic and commercial, is not coincidental: the cables follow navigational geography and both matter for the same reason.

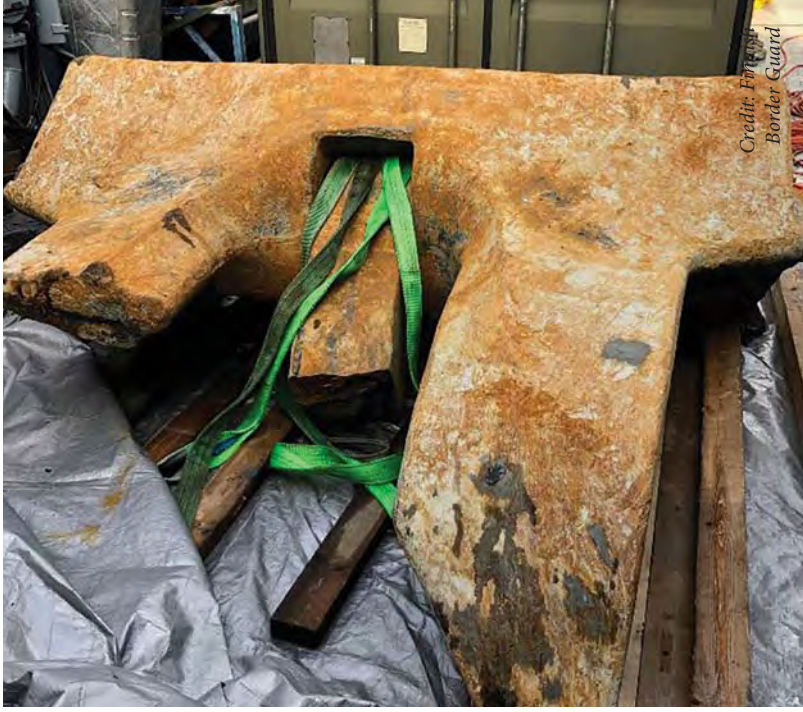
Canada's offshore energy infrastructure presents a parallel dimension. The Scotian Shelf, the Gulf of St. Lawrence and the Atlantic offshore zones host pipelines, wellheads and subsea production systems the disruption of which would have significant energy security consequences. Protection of this infrastructure has not been systematically integrated into the maritime security framework, leaving a gap between economic exposure and operational readiness.

The Arctic dimension is qualitatively distinct. Canada's 2019 extended continental shelf submission to the UN Commission on the Limits of the Continental Shelf asserts sovereign rights over vast areas of Arctic seabed. As sea ice retreats and traffic expands, cables for the region have moved from planning to construction. Far North Fiber, a 14,000-kilometre (about 8,700 miles) system routed from Europe through the Northwest Passage and the Bering Strait to Japan, is targeted for service in 2027 and federally supported fibre projects are underway in Nunavik and Nunavut.[7] Canada is acquiring seabed infrastructure in a theatre where it maintains minimal underwater monitoring capacity. The gap between sovereign aspiration and operational reality in the Arctic is a vulnerability in Canada's maritime security architecture.

The Rise of Grey-Zone Maritime Threats

Grey-zone conflict has moved from the academic literature into the operational calculus of naval commands.[8] Such activities remain below the threshold of armed conflict while advancing strategic objectives through ambiguity and deniability. Nowhere is the impact more consequential than in the subsea domain, where darkness, pressure, acoustic complexity and extreme depth create conditions uniquely hospitable to covert action.

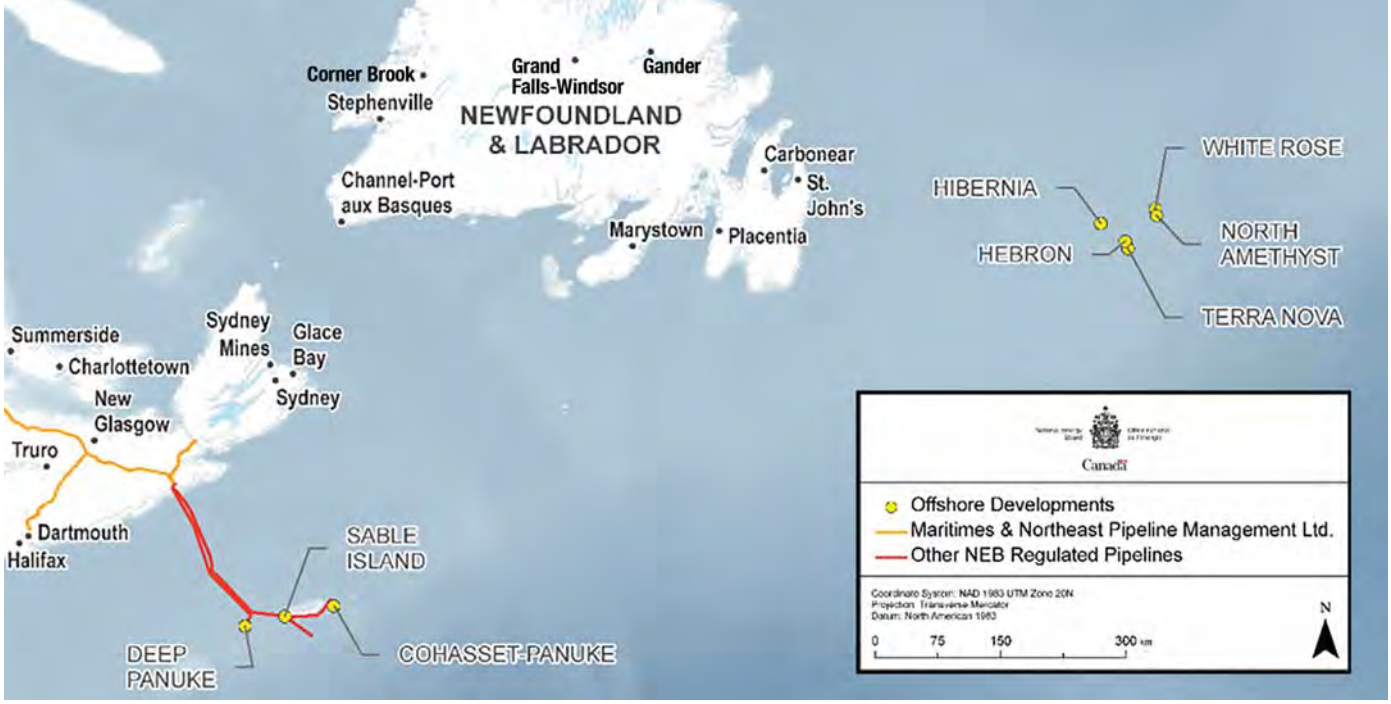
Russia's Main Directorate for Deep-Sea Research (GUGI) is the most developed state program for undersea grey-zone operations. GUGI operates modified nuclear submarines, deep-diving vessels and nominally civilian oceanographic research ships with submersibles able to work below the depths at which they can easily be monitored.[9] This is not an ad hoc capability but sustained investment in the ability to operate below detection levels.



The anchor recovered by Finnish authorities during the investigation on the damage to the Balticconnector pipeline.

The intelligence-gathering ship AGS *Yantar*, officially a hydrographic research vessel, has been tracked repeatedly by NATO navies near Atlantic cable corridors. Its submersible-equipped hull allows it to survey, map or interfere with seabed infrastructure under cover of legally protected civilian activity.[10] These transits form a systematic program the strategic objective of which is to put NATO's undersea infrastructure at risk in any future crisis, without technically committing an act of war.

The Nord Stream case showed that, regardless of the ultimate attribution, pipeline infrastructure stretching hundreds of kilometres across open seabed can be destroyed without warning, without triggering NATO Article 5 consultations and without establishing the evidentiary basis required for a calibrated response. The Balticconnector incident showed that even relatively unsophisticated means, such as an anchor and a commercial vessel, can achieve comparable strategic disruption while generating ambiguity about intent and attribution that paralyzes action in response.[11] The pattern is now routine rather than exceptional: *Yi Peng 3* severed two cables between Sweden and Lithuania in November 2024; the tanker *Eagle S* dragged its anchor some 90 kilometres (about 56 miles) through the Estlink 2 power cable and four telecommunications cables on Christmas Day 2024; and the cargo ship *Fitburg* was detained in the Gulf of Finland after it was suspected of dragging a broken anchor and damaging underwater telecommunications cables on 31 December 2025.[12] The lesson for any state actor seeking to coerce below the threshold of conventional deterrence is clear, empirically validated and operationally replicable.



Credit: National Energy Board

A 2017 map of offshore oil and gas activities in Atlantic Canada.

The deterrence problem runs deeper than capability gaps. Under the United Nations Convention on the Law of the Sea (UNCLOS), states must make damage to submarine cables a punishable offence (Articles 113-115), but UNCLOS provides no coercive enforcement mechanism and no basis for attributing state responsibility to operations conducted through nominally civilian platforms.[13] Beyond the territorial sea, jurisdiction over a ship rests principally with the flag state, which may have little incentive to exercise it. When Finland prosecuted the master and two officers of *Eagle S*, the Helsinki District Court dismissed the charges in October 2025 for want of jurisdiction, holding that the case belonged to the Cook Islands as flag state or to the crew's states of nationality. The Court of Appeal reversed this decision on 27 August 2026, finding that UNCLOS did not bar Finnish criminal jurisdiction.[14] That correction took 20 months, remains open to appeal, and occurred after the accused had left the country.

The operational point is simpler: a survey ship mapping a cable route in international waters commits no offence at all. The conduct becomes criminal only once the damage is done. Effective deterrence therefore requires the capability to detect and characterize subsea activity with enough fidelity to impose costs before damage occurs, not to investigate after it.

Limitations of Canada's Current Maritime Security Posture

Canada's maritime security architecture was designed for a different threat environment and has not been reconfigured for the subsea challenge. The RCN's surface fleet – six *Harry DeWolf*-class Arctic and Offshore Patrol Vessels, 12 *Halifax*-class frigates, and the future (up to) 15 *River*-class destroyers – offers surface presence but little subsea surveillance, infrastructure monitoring or underwater grey-zone deterrence. The *Victoria*-class submarine force, four boats bought from the United Kingdom in 1998, is Canada's only dedicated undersea capability. Availability, however, has run at one or two vessels at a time. Even were all four submarines in service, that is not the constant monitoring infrastructure protection requires. In July 2026 Canada named ThyssenKrupp Marine Systems' Type 212CD as the preferred supplier for the Canadian Patrol Submarine Project of up to 12 under-ice-capable boats, with contracting to conclude by the end of 2027 and first deliveries in the early 2030s.[15] The largest defence procurement in Canadian history will eventually triple the submarine arm, but it will not add a hull during the decade in which the infrastructure risk will be acute.

Our North, Strong and Free (ONSAF), Canada's April 2024 defence policy update, outlines a substantive commitment to defence: increased spending toward the NATO benchmark of 2% of GDP (which has now been met); investments in Arctic sovereignty and domain awareness; and a clearer posture for continental and maritime defence.[16] The Hague summit of June 2025 has already superseded this with a 5% target for 2035. Yet ONSAF's treatment of subsea infrastructure protection as a distinct operational mission remains under-developed relative to the scope of the threat. The document addresses Arctic maritime awareness and NORAD modernization with greater specificity than it addresses the seabed security problem, reflecting a persistent gap between the acknowledged importance of undersea threats and the institutional and doctrinal commitment needed to address them systematically.

The deeper structural problem has been institutional fragmentation, and on that point the ground has shifted. On 2 September 2025 an Order in Council transferred the Canadian Coast Guard (CCG), the agency with the largest fleet and longest continuous presence in Canadian waters,

from Fisheries and Oceans Canada to the Department of National Defence, where it remains a civilian, unarmed Special Operating Agency. The *Strengthening Canada's Immigration System and Borders Act*, which received Royal Assent on 26 March 2026, completed the change in law. It confirmed the Minister of National Defence as the responsible minister and added security to CCG services, expressly including security patrols and the collection, analysis and disclosure of intelligence.[17] In May 2026 the government committed $816 million over seven years to give that mandate substance, including a year-round maritime domain awareness hub in Iqaluit, four Arctic long-range marine radar sites along the Northwest Passage and Hudson Strait, and short- and medium-endurance aerial, surface and subsurface drones.[18]

This is real progress and it removes the machinery-of-government objection that stalled Canadian maritime security thinking for two decades. What it does not do is create a subsea infrastructure protection mission. The new authority is framed around patrols, surveillance and intelligence sharing on the surface and nothing in it makes anyone responsible for the seabed. The Marine Security Operations Centres in Halifax and Victoria coordinate surface domain awareness but are not integrated with subsea monitoring and hold no mandate for intelligence fusion in the water column. Canada can see the ship. It still cannot reliably see what the ship is deploying beneath it.

Building a Canadian 'Seabed-to-Space' Security Framework

Doctrinal reorientation matters as much as capability investment. The recommendations below are designed for a middle power with limited resources, a strategically consequential location, and legal and alliance commitments. They are cumulative rather than sequential – each reinforces the others and together they constitute a posture Canada can build toward incrementally within the spending trajectory ONSAF has established.



Credit: Royal Navy, UK MOD Crown copyright 2025

*The Russian hydrographic vessel **Yantar** is seen here being escorted by the Royal Navy Type 23 frigate HMS **Somerset** on 5 November 2025 near the United Kingdom.*

Integrated Underwater Surveillance Architecture

Canada should develop persistent, layered underwater surveillance coverage of its critical maritime approaches, beginning with the North Atlantic gateway to the Atlantic provinces and extending into Arctic chokepoints (and the Pacific approaches). The US Navy's Integrated Undersea Surveillance System (IUSS), which combines fixed hydrophone arrays with mobile and expendable sensors across multiple ocean basins, is the baseline against which Canadian contributions should be designed.[19] Canada should negotiate enhanced access to IUSS data as part of ongoing NORAD modernization, contributing monitoring capacity at nodes near Canadian territory in exchange for allied network access. This arrangement would multiply Canadian situational awareness at a fraction of the cost of independent system development, a formula appropriate to a middle-power defence budget navigating credible capability requirements and fiscal constraints simultaneously.

Autonomous Underwater Vehicles as the Surveillance Backbone

Autonomous Underwater Vehicles (AUVs) now provide a practical and affordable basis for long-term monitoring from the sea. Continuous patrols around cable corridors and infrastructure nodes offer the persistent awareness crewed submarine operations cannot achieve cost-effectively. Other navies have invested in AUVs for infrastructure monitoring, providing procurement models Canada can adapt.[20] The CCG's newly funded subsurface drones are the obvious first vehicle.

A Canadian program should be presented as an investment in maritime domain awareness rather than as a substitute for the submarine program, which protects political buy-in across the defence spectrum and allows procurement through existing domain awareness mechanisms. The Artificial Intelligence- (AI) based sensor processing used in allied programs would flag GUGI-style survey operations without constant crewed supervision.

Deepened NATO Seabed Partnership

Canada should take an active role at NATO's Maritime Centre for the Security of Critical Undersea Infrastructure, established at Allied Maritime Command Northwood in the UK in 2023.[21] The centre serves as the primary alliance coordination mechanism for subsea infrastructure protection doctrine and intelligence fusion. Active participation, not nominal membership, means dedicated intelligence-sharing on seabed anomalies, joint exercises

in infrastructure protection and bilateral arrangements under NORAD that create a shared operating picture for cable corridors making landfall in Canada.

Two developments make this urgent rather than aspirational. Task Force X-Baltic, NATO's autonomous seabed surveillance experiment, moved in February 2026 from experimentation to nationally owned capability, with an Arctic counterpart following. As well, the enhanced vigilance activity Arctic Sentry, launched the same month under Joint Force Command Norfolk, has brought allied Arctic activity under a single operational approach.[22] Canada, which supports Arctic Sentry through NORAD and *Operation Nanook*, is well placed to make the undersea dimension its distinctive contribution and poorly placed to do so without sensors of its own. The Five Eyes framework already operates at the relevant classification levels and should be extended explicitly to undersea threat intelligence and attribution.

Joint RCN-Canadian Coast Guard Operational Mandate

The legislative step this recommendation would have called for a year ago has been taken, but what is missing is the mission. Canada should define critical subsea infrastructure protection as a named joint DND-CCG task, with protocols for surveillance, incident response and graduated escalation. It should fit CCG science and patrol vessels with passive acoustic sensors and standardized AUV launch and recovery systems, multiplying monitoring presence along cable corridors without naval fleet expansion. The amended *Oceans Act* already supplies the authority, so vessels running existing oceanographic programs can double as seabed monitoring platforms without altering their civilian character or their status under international law.[23] The instruments now exist. The tasking does not.



Credit: Kym Smith

A prototype 'Ghost Shark' autonomous undersea vehicle is seen at Fleet Base East in Sydney during the 10 September 2025 announcement of Australia awarding a contract to Anduril for a fleet of such vessels.

AI-Supported Maritime Domain Awareness Integration

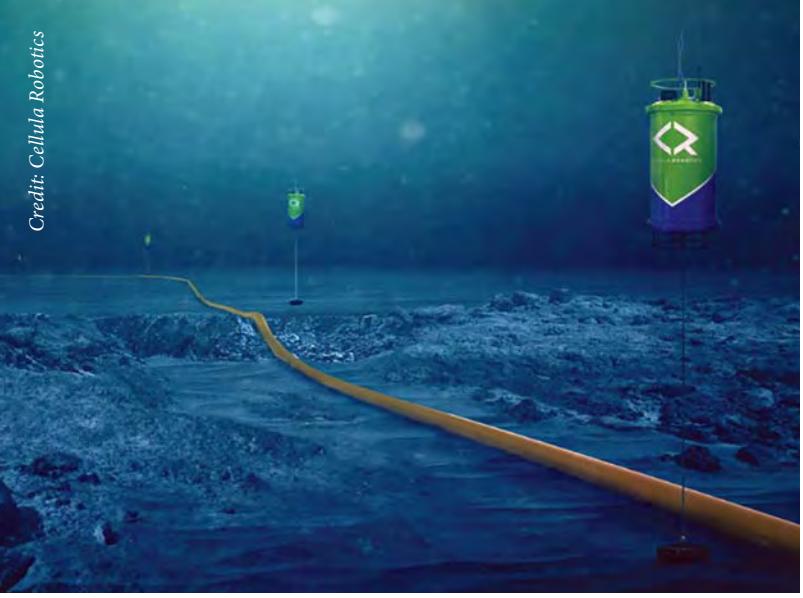
Canada's maritime domain awareness architecture should integrate undersea, surface and overhead surveillance into a unified picture through an AI-assisted fusion platform. RADARSAT Constellation Mission imagery, Automatic Identification System (AIS) data, passive acoustic monitoring and AUV sensor outputs are a technically achievable near-term synthesis. Allied navies already use AI to detect anomalies in datasets, identifying patterns of vessels loitering near cable routes, AIS spoofing and unusual acoustic signatures near infrastructure nodes that conventional analysis might miss. The Joint Expeditionary Force's Nordic Warden, which risk-scores vessels entering areas of interest around undersea infrastructure, is a working example rather than a concept.[24] Integrating comparable capability through the MSOCs would turn domain awareness from a surface-oriented coordination platform into a multi-domain enterprise capable of identifying grey-zone signatures before they escalate to incidents.

Arctic Sensor Network as Strategic Priority

Canada should treat Arctic underwater sensor development with the urgency it applies to NORAD radar modernization. The four new Arctic marine radar sites announced in May 2026 will watch the surface; nothing announced to date watches beneath it. A distributed passive acoustic network, deployed incrementally along chokepoints as infrastructure operations permit, would serve both sovereignty affirmation and security monitoring. ONSAF's Arctic domain awareness commitments provide the political foundation; what is required is programmatic investment rather than continued rhetoric. Norway and the United States both offer alliance-embedded models that do not require Canada to begin from a standing start. The cost of entry is contribution, not construction.

Dedicated Doctrine for Subsea Infrastructure Security

Capability without doctrine performs below its potential. Canada needs an operational framework for subsea infrastructure security that defines threat thresholds and sets graduated response protocols for ambiguous attribution, and integrates cyber and physical protection into one architecture. The doctrine must address grey-zone scenarios explicitly – the survey vessel loitering near a cable corridor, the anomalous acoustic contact near an offshore energy node, the unexplained pipeline fault with no visible surface cause – and authorize protective and investigative measures without requiring conclusive attribution first. That is a departure from Canada's reactive posture and precisely the departure the operational environment now demands.



Subsea Sentinel surveillance sensors are seen anchored near an underwater cable in this computer-generated graphic provided by the manufacturer, Cellula Robotics.

Conclusion

The ocean floor is no longer a domain Canada can treat as beneath strategic notice. The Balticconnector and Nord Stream incidents are not European anomalies; they demonstrate a form of infrastructure coercion to which Canada's maritime geography, seabed assets and NATO obligations are exposed. A middle power cannot achieve undersea dominance, but it can and *must* build the awareness, partnership architecture and doctrine to deter, detect and respond to threats in the subsea domain.

The 'seabed-to-space' framework proposed here is neither extravagant nor unrealistic. Integrated passive acoustic surveillance, persistent AUV monitoring, enhanced NATO seabed partnership, a defined joint RCN-CCG seabed mission built on the CCG's new statutory security role, AI-enabled domain awareness, Arctic sensor investment, and dedicated doctrine constitute a coherent program achievable within the spending trajectory the government has established. Much of the machinery is already in place: the CCG sits inside the defence portfolio; the submarines have been chosen; and money has been pledged. What is missing is the decision to point any of it at the seabed. These investments do not require Canada to become a great maritime power; they require it to become a competent one for the era in which it operates.

Maritime power in the 21st century is measured not just by hulls on the surface but by how well a state can understand, contest and respond to threats across all three maritime dimensions – above the sea, on it and beneath it. Canada's naval identity, sovereign obligations and alliance commitments all require that its security posture reflect that reality.

Notes

1. Finnish National Bureau of Investigation, press statement identifying the Hong Kong-registered vessel *NewNew Polar Bear* as the primary suspect, April 2024; Reuters, "Finland Points to Chinese Ship in Baltic Pipeline Probe," 26 April 2024. Chinese authorities concluded in August 2024 that the damage was accidental; the master pled not guilty in a Hong Kong court, on 11 February 2026.
2. German Federal Public Prosecutor, charges filed against Serhii K. in connection with the September 2022 Nord Stream explosions, July 2026.
3. TeleGeography, *Submarine Cable Map* (Washington, DC: PriMetrica, 2025). See also International Cable Protection Committee (ICPC), Annual Report on Cable Faults and Statistics (various years).
4. NATO, *Strategic Concept 2022*, Brussels, June 2022.
5. NATO, "The Hague Summit Declaration," 25 June 2025, paragraph 3; NATO, "The Ankara Summit Declaration," 8 July 2026. No new Strategic Concept has been adopted since Madrid in 2022.
6. TeleGeography, *Submarine Cable Map*.
7. Far North Fiber, project information, 2026; on Canadian Arctic fibre projects see Alexander Dalziel, "Critical Resilience: Russia, Hybrid Threats, and Subsea Fibre-Optic Cables in Canada's Arctic," Ottawa: Macdonald-Laurier Institute, June 2024.
8. Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: Strategic Studies Institute, US Army War College, 2015), pp. 19-38. See also Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007).
9. See International Institute for Strategic Studies (IISS), *The Military Balance 2026* (London: Routledge, 2026), sections on Russian naval special forces and deep-sea research capabilities.
10. H.I. Sutton, reporting on Russian undersea intelligence activities including tracking of the AGS *Yantar*, *US Naval Institute News* (various, 2017-2024); UK Ministry of Defence, statements on the tracking of Russian intelligence vessels in Atlantic and Mediterranean cable corridors (various dates, 2017-2023).
11. Finnish National Bureau of Investigation, Balticconnector investigation, 2023-2024.
12. *Ibid*.; NATO Allied Command Operations, launch of Baltic Sentry, Helsinki, 14 January 2025; Finnish and Swedish investigations into the *Yi Peng 3* (November 2024), *Eagle S* (December 2024) and *Fitburg* (December 2025) incidents. Baltic Sentry is the model most directly transferable to Canada.
13. United Nations Convention on the Law of the Sea (UNCLOS), Articles 113-115. Article 113 requires states to criminalize cable damage; Articles 114-115 address specific civil liability provisions.
14. Helsinki District Court, judgement of 3 October 2025 (jurisdiction declined); Helsinki Court of Appeal, judgement of 27 August 2026 (jurisdiction affirmed, case remitted), subject to any further appeal to the Supreme Court.
15. Government of Canada, announcement of TKMS as preferred supplier for the Canadian Patrol Submarine Project, 6 July 2026.
16. Government of Canada, *Our North, Strong and Free: A Renewed Vision for Canada's Defence* (Ottawa: DND, April 2024).
17. Order in Council transferring the Canadian Coast Guard to the Department of National Defence, 2 September 2025; *Strengthening Canada's Immigration System and Borders Act* (Bill C-12, 45th Parl., 1st Sess.), Part 4, amending the *Oceans Act*, R.S.C. 1985, c. O-2 (new s. 41(1)(f) and s. 41.1), Royal Assent 26 March 2026.
18. DND, "Minister McGuinty Announces $816 Million Investment to Strengthen Canada's Maritime Security," News Release, Iqaluit, 22 May 2026.
19. United States Navy, Integrated Undersea Surveillance System (IUSS), documented in US Congressional Research Service and Congressional Budget Office publications on naval undersea warfare. For Canada-US undersea cooperation, see DND, "NORAD Modernization Program," documentation 2022-2024.
20. Norwegian Defence Research Establishment, publications on autonomous underwater systems for naval applications; Australian Department of Defence, "Integrated Investment Programme 2024," Canberra, 2024, lists autonomous maritime systems investment priorities.
21. NATO Allied Maritime Command, "NATO Establishes Maritime Centre for the Security of Critical Undersea Infrastructure," Press Release, Northwood, UK, 2023.
22. NATO Allied Command Transformation, Task Force X-Baltic, letter of intent of eight Allies to move to Phase II, February 2026; SHAPE, "Arctic Sentry," enhanced Vigilance Activity launched 11 February 2026 under Joint Force Command Norfolk; DND, "Canadian Armed Forces launch Operation Nanook-Tuugaalik in Canada's Arctic," News Release, August 2026.
23. *Oceans Act*, R.S.C. 1985, as enacted by the *Strengthening Canada's Immigration System and Borders Act*, Part 4. The authority extends to security patrols and to the collection, analysis and disclosure of information or intelligence, without conferring law enforcement powers.
24. See, for example, UK Ministry of Defence, "Defence AI and Automation Programme," publications on maritime domain awareness (2022-2024); NATO Allied Command Transformation, "Warfare Development Agenda 2024"; Government of the UK, "Joint Expeditionary Force Activates UK-led Reaction System to Track Threats to Undersea Infrastructure," 6 January 2025.

C.A.M. Al Wahi is a Bangladeshi lawyer and law of the sea researcher affiliated with the Bangladesh Centre for Ocean Law and Policy.